State of Indiana Policy and Standards

Data Encryption

Standard ID
IOT-CS-SEC-003

Published Date
10/3/2016

Effective Date
10/3/2016

Last Updated
9/28/2016

Next Review Date
9/28/2017

Policy
08.0 Data Security (PR.DS)
- 08.1 PR.DS-1
  - 08.1.1 Data-At-Rest
- 08.2 PR.DS-2
  - 08.2.1 Data-In-Transit

Purpose
To identify when State data must be encrypted and the associated encryption requirements. Encryption can render data unreadable in the event of loss, theft or interception, reducing the risk of leakage and/or breach of information.

Scope
IOT Supported Entities

Statement
Protection of information is critical to State security and operations. Below are encryption requirements for confidential, private and sensitive data (i.e. Federal Tax Information, Credit Card Numbers, Personally Identifiable Information, Passwords, or other information not meant for public consumption):

-Information shall not be sent over the internet (e.g., email, ftp, etc.), via remote access or transmitted over public or external networks unless the data is encrypted
-Information shall be encrypted in transit, whether being transmitted internally or externally
-Information shall be encrypted at rest. Information at rest refers to the state of information when it is located on a primary or secondary storage device (server, portable devices, solid state drive, etc.)

The above requirements require strong cryptography and security protocols. All encryption mechanisms and configurations must have a validated Federal Information Processing Standard (FIPS) 140-2 cryptographic module and meet National Institute of Standards and Technology (NIST) 800-131A encryption requirements.

All State issued devices, such as laptops and phones must have IOT approved encryption technologies installed and turned on prior to distribution. Employees shall not install any encryption software not validated and approved by the IOT Security Team.

Roles
All Personnel

Information Asset Owners/System Owners

Responsibilities
All personnel must be aware of data classification and encryption requirements for their agency. Information Asset Owners/Systems Owners shall confirm data is encrypted to the appropriate level based on control standard requirements.

Management Commitment
Management shall ensure that data requiring encryption meets the requirements of this control standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary to turn on encryption. Further, agencies shall coordinate with necessary regulatory bodies to confirm encryption requirements are met.

Compliance
Asset encryption settings may be reviewed or scanned for compliance with this standard at any time. Assets that are found in non-compliance may be removed from the network.

Exceptions
If it is not technically possible to meet this standard, agencies must submit an exception for review by the Director of Risk & Compliance and State CISO.

Associated Links
FIPS 140-2
NIST 800-131A